BEST PRACTICES GUIDE

Given the current context and in order to protect the confidentiality of clients' personal information, iA has prepared this Guide to ensure that the distributors with whom it does business follow best practices in carrying out their professional activities, including remote sales and service provision.

In the course of your professional activities, it is important to remember that it is your responsibility to maintain the confidentiality of your clients' personal information, regardless of the tools or means of communication used.

Recording of videoconferences not allowed

Videoconferences may not be recorded. Even though Zoom and Skype offer this feature, you are not allowed to make such recordings.

Confidential and secure place to conduct your business

In the course of your business activities, you may have to discuss confidential information with clients or ask them to provide you with documentation containing confidential information, particularly when verifying their identity with photo ID. Make sure you are in a suitable location where no one can see or hear the confidential information.

Sharing and storing of personal information

Files may not be shared via platforms such as Skype and Zoom. Neither may unsecured email, USB keys or external hard drives be used to exchange or store confidential client information. None of these tools are secure.

Skype and Zoom also have a chat feature, providing written instant messaging between two or more people. This chat history is saved on Skype's and Zoom's servers, so it is essential that confidential information not be shared in the chat box.

Security of your workstation

A quick reminder about best practices to keep your workstation secure. Ensure that your computer is receiving security updates from the manufacturer (Microsoft, Apple or other). Also ensure that your antivirus program is functional and up-to-date, and that your computer takes a password to unlock.

Using your workstation outside your usual workplace and iA's Wi-Fi may expose you to greater security risks. For this reason, it is important to use your computer responsibly and carefully and only for business purposes. Your computer should always be locked when you are not working on it, whether at the office or at home.

iA Financial Group

INVESTED IN YOU.

ia.ca

SRM390-20A